March 5 - March 11, 2018

Check Point SOFTWARE TECHNOLOGIES LTD.

YOUR CHECK POINT

THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Researchers have recently discovered an APT operation that has been running since at least 2012, infecting hundreds of thousands of victims from the Middle East and Africa with a malware dubbed Slingshot. The attack starts with exploiting an unknown vulnerability in Mikrotik routers, then replacing a DDL (dynamic link library) file with a malicious one used to infect linked computers.

- Following the recent exposure of the ability to use Memcache to enhance DDoS attacks, an increase was discovered in such attacks, with nearly 15,000 launched against 7,131 unique targets in the last ten days.

  Check Point IPS blade provides protection against this threat *(Memcached Web-Servers Network Flood Denial of Service)*

- Security researchers have warned against two new cryptomining campaigns attempting to infect unpatched Windows, Apache Solr, and Redis servers. Once installed on the system, the malware runs a cryptocurrency mining script on the host, while attempting to self-propagate by scanning for additional vulnerable servers within the network.

  Check Point IPS blade provides protection against this threat *(Apache Solr xmlparser XML External Entity Expansion Remote Code Execution (CVE-2017-12629); Apache Struts REST Plugin XStream Deserialization Remote Code Execution (CVE-2017-9805); Microsoft Windows Eternal* SMB Remote Code Execution; Microsoft Windows SMB Information Disclosure (MS17-010: CVE-2017-014*))*

- A new report reveals the use of ISPs in the distribution of malware in Turkey, Egypt and Syria, in what seems to be state-run attacks. The ISPs were injecting spyware and crypto-miners to home users.

  Check Point IPS blade provides protection against this threat *(Multiple Websites Mine Cryptocurrencies CPU Hijacking; Malicious Crypto Miner Downloader)*

- Security researchers have warned that the North Korean APT group Hidden Cobra is targeting large financial institutions in Turkey. The attackers are sending a targeted fraudulent email with a malicious Word document attached, utilizing a newly discovered Flash vulnerability.

  Check Point IPS blade provides protection against this threat *(Adobe Flash Player Use After Free (APSB18-03: CVE-2018-4878; Suspicious Microsoft Office File Archive Mail Attachment; Suspicious Executable Mail Attachment)*

VULNERABILITIES AND PATCHES

- A critical remote code execution vulnerability has been discovered in the mail transfer agent (MTA) 'Exim', affecting 56% of all of the Internet's email servers. The vulnerability may allow an attacker to trick the Exim email server into running malicious commands without the need of authentication.
- Google has released its most recent version of Chrome, Chrome 65, with 45 security fixes, among which a prevention of tab-under redirects —when a web page opens links in new tabs and redirects the old tab to a new URL, a method widely used for both advertising and malvertising.

  Check Point IPS blade provides protection against this threat *(Google Chrome Object Create Type Confusion; Google Chrome Out Of Bound Read; Google Chrome Type Confusion; Google Chrome Write Barrier Elimination)*
- Cisco has released patches for vulnerabilities impacting several of its products, Cisco Prime Collaboration, Cisco Secure Access Control System and Cisco Web Security Appliance.
- Intel has released further patches for the Spectre/Meltdown vulnerability, this time for its Ivy Bridge and Sandy Bridge processor families.

  Check Point IPS and Anti-Bot blades provide protection against this threat *(Meltdown/Spectre Multiple Browsers Speculative Execution (CVE-2017-5715; CVE-2017-5753; CVE-2017-5754; Trojan-Ransom.Win32.Spectre)*

THREAT INTELLIGENCE REPORTS

- A new intelligence report sheds light on the NSA cyber tools leaked by the "Shadow Brokers" threat group. According to the report, along with the previously-reported tools and exploits, a collection of scripts and scanning tools has also been leaked, allegedly used by NSA in order to detect APTs and threat groups active in the wild. The scanning tools are believed to have helped the NSA to track over 45 different APTs.
- Security researchers have detected new variants of Hacking Team's spy software in the wild. The surveillance company, infamous for allegedly providing advanced cyber-espionage tools for rogue regimes, had kept a low profile after being hacked in 2015.

For comments, please contact: TI-bulletin@checkpoint.com